ATTORNEY DOCKET No.
GATEP002

PATENT APPLICATION

ELECTRONIC FILE PROTECTION USING LOCATION

INVENTOR: Roger R. Dube
2655 NW 29th Drive
Boca Raton, FL 33434
U.S. Citizen

ASSIGNEE: Gate Technologies International, Inc.
3700 Airport Road, Suite 307
Boca Raton, FL 33431

MARTINE & PENILLA, LLP
710 Lakeway Drive, Suite 170
Sunnyvale, CA 94085
Telephone (408) 749-6900

For example, the Internet, intranets and extranets are used to store, analyze and transmit information between and within organizations, and permit interactive, local, national or global communication on a real-time basis. Moreover, these networks are now used for electronic business-to-customer retail commerce and for electronic business-to-business commerce of all types.

Electronic files today are easily copied and transmitted widely throughout the world in a largely uncontrolled and nearly instantaneous fashion. Multiple computers connected through a variety of local and global networks can share information through the copying and electronic delivery of files. Further, a variety of tools have been developed to facilitate file sharing and communication, such as Virtual Private Networks ("VPN's"), Peer to Peer ("P2P") software, various instant messaging packages as well as others. Due to the wide availability of this software, computer files of all types are shared with increasing frequency. Moreover, the continuing reduction in the price of storage devices such as disk drives further encourages this activity, since the cost of local storage does not suppress the benefit obtained by having immediate and continual access to the data.

As a result, there is a strong and pressing need for a complete solution to the protection of copyrighted information in this electronic environment. Owners of copyrighted digital data, such as video files, audio files and reports, are very concerned about the proliferation of world wide sharing of files, since this often constitutes a direct violation of copyright laws and leads to the erosion of revenue due the owner. Some sharing engines caused such concern about copyright infringement that legal battles have risen to the highest courts in the land in an attempt by copyright owners of audio data to

places the burden upon the owner to locate and then prosecute people holding illegal copies. The lack of tools to track the distribution path by which these copies were transmitted does not provide any assurances that such distribution will be stemmed by the prosecution activity. The ease with which keys can be distributed or posted in newsgroups gives further pause to copyright owners. Hence, a solution is needed in which copyrighted materials can be transmitted to an authorized purchaser with confidence that the file cannot be distributed in any usable fashion.

To address this issue, a variety of very strong encryption technologies have been developed over time. The strongest of the encryption technologies, public key encryption, employs dual-key systems in which each party has a public key that is widely distributed, and a private key that is kept secret to the user on his machine. Specifically, using public key infrastructure ("PKI") encryption, digital messages are encrypted and decrypted using ciphers or keys. Figure 1 is an illustration showing a conventional public and private key pair 100. The public and private key pair includes a public key 102 and a private key 104. Each user of the system has a public key 102 and a private key 104 and must know the public key 102 of the intended recipients of its messages. In general, a message is encrypted and sent by a sender using the recipient's public key 102 and is then received and decoded by the recipient using his private key 104, as discussed in greater detail next.

Figure 2 is an illustration of a conventional PKI system 200. In Figure 2, two network computer users, Alice 202 and Bob 204, each have their own public and private key pair. Specifically, Alice 202 has a public and private key pair comprising a public key 206 and a private key 208. Similarly, Bob 204 has a public and private key pair comprising a public key 210 and a private key 212. The private keys 208 and 212 are

202 has a public and private key pair comprising public key 206 and private key 208, and Bob 204 has a public and private key pair comprising public key 210 and private key 212. In addition, Cindy 302, the middleman, has a public and private key pair comprising public key 304 and private key 306. If Cindy 302 can intercept a transmission between Bob 204 and Alice 202, she can trick them into using her public key 304. In this attack, the attacker intercepts the transmission of a public key and replaces it with the attacker's false key, thereby effectively replacing the true sender as the trusted party. This enables the attacker to send, receive and decode messages intended for the original legitimate user.

For example, during a "man-in-the-middle" attack, Cindy 302 intercepts Alice's public key 206 and replaces it with Cindy's public key 304. Similarly, Cindy 302 intercepts Bob's public key 210 and replaces it with Cindy's public key 304. Bob 204 and Alice 202 each believe they have each other's public key, however, they actually have Cindy's public key 304. Later, during encrypted transmissions, both Alice 202 and Bob 204 unknowingly use Cindy's public key 304 in conjunction with their respective private keys to encrypt messages to each other, which are actually intercepted by Cindy 302. Cindy 302 can decrypt the messages using her private key 306, and further, re-encrypt the messages using Cindy's private key 304 and the proper recipient's public key 206 and 210.

As deployed today, public key encryption cannot and does not have any means to authenticate the identities of either party involved in a transmission. The parties must rely upon trust or some other means of authentication in order to be certain that the identity of the other party is indeed the person with who they wish to communicate.

The strength of this public key encryption technology is state of the art today, with

locations. This is practical only for application specific satellites and does not provide a means for authentication of the user's location.

In U.S. Patent No. 5,343,529, Goldfine et. al. describe a system by which a user requesting access to data presents such a request to a server. The server then transmits a session-specific userid to the user, and simultaneously calculates a hash code based on that userid. The user calculates a hash code based on a pre-determined algorithm, and sends the code back to the server. If the two hash codes match, the user is considered authentic and access is allowed. The security of this system is only as good as the secrecy of the predetermined algorithm (static entropy), and does not employ location or dynamic entropy to further authenticate the user.

RO 10/725/0

In U.S. Pat. No. 5,640,452, Murphy describes a system by which a receiver that receives encrypted television transmissions will only operate within a physical range around its pre-set location. The system employs a GPS receiver operating in close proximity to the receiving antenna. If the current location as received by the GPS unit is within an acceptable range of coordinates that have been stored within the antenna's local electronics, the circuitry sends an enabling pulse to a decryption chip which then decodes the received transmissions. The system is susceptible to short-circuiting the enabling line to enable the decryption chip at all times and failure of the GPS unit. Moreover, it does not involve a challenge/response process for authentication of the user or his location, nor does it employ dynamic entropy for enhanced security.

In view of the forgoing, there is a need for systems and methods that provide self-protecting electronic files. The self-protecting electronic files should protect themselves based on a set of variables defined by the copyright owner at the time of authentication

SUMMARY OF THE INVENTION

Broadly speaking, the present invention fills these needs by providing electronic file protection using location and other entropy factors. In one embodiment, a method for protecting electronic files is disclosed. Environment information regarding a computer is obtained, wherein the environment information includes data concerning an operating environment of the computer. Based on the environment information, an encryption key is generated and an electronic file is encrypted using the encryption key. A decryption key can also be created based on environment information, wherein the decryption key can be utilized to decrypt the electronic file. In addition, the environment information can include location information of the computer, drive information regarding a drive wherein the electronic file will be stored, and time information specifying access duration.

Another method for protecting electronic files is disclosed in a further embodiment of the present invention. An electronic file is stored that is encrypted using an encryption key. The encryption key is generated using a first environment profile that includes data concerning an operating environment of the computer. A second environment profile of the computer is obtained, again based on a current operating environment of the computer. A decryption key is generated based on the second environment profile, and the electronic file is decrypted using the decryption key. The encryption key and the decryption key can be further based on a passcode received from a user. In this aspect, the first environment profile can be appended to the passcode to generate the encryption key and the current environment profile can be appended to the passcode to generate the decryption key. Generally, the decryption key cannot decrypt the

BRIEF DESCRIPTION OF THE DRAWINGS

The invention, together with further advantages thereof, may best be understood by reference to the following description taken in conjunction with the accompanying drawings in which:

Figure 1 is an illustration showing a conventional public and private key pair;

Figure 2 is an illustration of a conventional PKI system;

Figure 3 is an illustration showing a PKI system compromised by a middleman;

Figure 4 is an illustration showing a client computer system that utilizes GPS data to facilitate authentication, in accordance with an embodiment of the present invention;

Figure 5 is a timing diagram illustrating timing signals from a satellite of a GPS system;

Figure 6 is a block diagram showing a real-time digital authentication system, in accordance with an embodiment of the present invention;

Figure 7 is a flowchart showing a method for initializing a real-time digital authentication system, in accordance with an embodiment of the present invention;

Figure 8 is a flowchart showing a method for obtain summary data including GPS entropy data, in accordance with an embodiment of the present invention;

Figure 9 is a flowchart showing a method for creating a Digital Certificate using obtained client summary information, in accordance with an embodiment of the present invention;

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

An invention is disclosed for electronic file protection using location and other entropy factors. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent, however, to one skilled in the art that the present invention may be practiced without some or all of these specific details. In other instances, well known process steps have not been described in detail in order not to unnecessarily obscure the present invention.

In order to provide a thorough understanding of the present invention, two devices are defined. The first device, a "User Card", resides on a client computer system, disk drive or other electronic device that is employing the present invention. The term "card" is used figuratively and is not meant to limit the implementation or packaging of the present invention in any way. This User Card may reside entirely within a host device, may be plugged in to a host device, or otherwise electronically attached to the device through any one or more attachment means, such as PCMCIA connector, serial port, parallel port, wireless connection, or other means. It will be apparent to those skilled in the art that these attachment means are intended to present examples and not intended to limit the present invention in any way. The second device, the "System Card", resides on the server computer system or other host which is controlling access to information and requires authentication of a user.

Figures 1, 2, and 3 have been described in terms of the prior art. Figure 4 is an illustration showing a client computer system 400 that utilizes global positioning satellite (GPS) data to facilitate authentication, in accordance with an embodiment of the present

The timing signals 404 include encoded time and date information that can be extracted by the User Card 410 and/or the client computer 409, as will be apparent to those skilled in the art. Further, by triangulation of signals from three of the satellites 410, the User Card 410 can pinpoint the current geophysical location of the computer anywhere on earth, generally to within a few meters. However, variations in the ionosphere and atmosphere 406 due to weather, barometric pressure, solar activity, and other variable and unpredictable parameters cause the purity of the timing signals 404 to fluctuate. In particular, the variations in the ionosphere and atmosphere cause unpredictable delays in the timing signals 404. To compensate for these variances, each satellite 402 of the GPS system transmits two timing signals 404 at two different frequencies (L1 and L2).

Figure 5 is a timing diagram illustrating timing signals 404 from a satellite of a GPS system. The timing signals 404 include a first timing signal 404a at a first frequency and second timing signal 404b at a second frequency. As Figure 5 illustrates, the first and second timing signals 404a and 404b are offset from each other as a result of atmospheric variances. The delay of a radio signal is inversely proportional to the square of the carrier frequency (i.e. L2 will be delayed more than L1) and proportional to the total number of electrons along the path from the satellite to the receiver. The total number of electrons will vary according to the current solar activity, time of day (at the receiver), and longitude and latitude of the receiver. It is known to one practiced in the art that by measuring the delay between signals L1 and L2 from a particular satellite, one can calculate the effect due to the ionosphere and troposphere and correct for the variation, thereby improving positional accuracy. To compensate for the atmospheric variances, the embodiments of the present invention normalize the first and second timing signals 404a

Entropy is a highly effective means of achieving strong encryption. In addition to the timing signal delay discussed above, a "secret" is another example of an entropy element that the embodiments of the present invention utilize to increase system security. A "secret", as used in the industry, is a piece of information known only to the user 408 or specific local User Card 410. A properly chosen "secret" makes it very difficult, if not impossible, for an outside party to guess the value of the secret. An example of a "secret" is a personal identification number (PIN) or passphrase. Because the introduction of such a non-predictable item adds randomness and uncertainty to the system, such a technique is said to add entropy to the system, resulting in dramatically increased overall security.

Referring back to Figure 4, embodiments of the present invention can utilize four or more satellites 402 when acquiring timing signals 404. By using additional satellites 402, consistency can be checked and any errors discarded. Moreover, the embodiments of the present invention utilize various signal processing techniques and weak signal extraction to provide strong signal acquisition deep within buildings or in urban canyons, where the visibility of the sky is limited or missing entirely. Exemplary signal processing techniques utilized by embodiments of the present invention include Differential GPS (DGPS), Wireless Aided GPS (WAG), repeater systems, and methods of phase sensitive detection, each of which are known to those skilled in the art.

Figure 6 is a block diagram showing a real-time digital authentication system, in accordance with an embodiment of the present invention. The real-time digital authentication system includes User Card 410 on a client computer 409 and System Card 600. As discussed in greater detail subsequently, the real-time digital authentication system employs a combination of remote, personal, and local elements in such a manner

authentication operations will include biometric data, the method 700 proceeds to operation 706. Otherwise, the method 700 continues with operation 708.

In operation 706, biometric characteristics are obtained from the user. Each user establishes a personal profile of their biometric characteristics, generally, by submitting themselves to a biometric scanning device. This profile is used to control the user's access to the authentication system or machine, as is preferred by the particular system or application employing the device. A preferred embodiment will require that the user interact directly with the biometric access device or other input/output interface that resides solely on the User Card or the user's computing device during the authentication process. This forces the user to be physically present at their machine during the authentication process, and avoids masquerading or other remote access attempts using various remote control programs available on the market today.

A passphrase or PIN is obtained from the user in operation 708. Generally, the passphrase or pin number is known only to the individual user and is not disclosed to others. Referring back to Figure 6, a summary of the passphrase or PIN, or a brief hash sequence of the biometric characteristics, or combination of these is stored on the System Card 600, shown as PIN data 602 within the profile 606 in Figure 6. If desired, a system administrator can confirm the user's identity. The system administrator can further "seal" to the profile by indicating who the administrator is, the time, date, and location of the initialization, and any additional unique information required by the application.

RD 10/29/c

Turning back to Figure 7, a decision is then made as to whether mobile access will be available to the user, in operation 710. Mobile access allows authentication of the user when the user is not at a registered location. If mobile access will be available to the

stored in the client random number stack 612 and client delay stack 614 of the User Card 410 at the time of initialization.

Referring back to Figure 7, in operation 718, a public and private key pair is generated for the User Card 410 on the client computer 409. As shown in Figure 6, the client public key 616 and client private key 618 are both stored on the User Card 410. In addition, the client public key 616 is stored in a database on the System Card 600. The client public key 616 and client private key 618 are used for encryption, as discussed in greater detail subsequently.

The system default public key 620 is then stored on the User Card 410, as shown in operation 720 of Figure 7. In the real-time digital authentication system of Figure 6, the System Card stores a system default public key 620 and a system default private key 622. The system default private key 622 is kept confidential on the System Card 600. However, the system default public key 620 is distributed to the User Card 410 that will access information or data on the server computer through the System Card 600. Post process operations are then performed in operation 722. Post process operations can include additional verification of the user identity, initialization of additional users, and other post process operations that will be apparent to those skilled in the art.

When the user desires to authenticate a file, electronic transaction, or other form of electronic action, the commencement of the authentication process can occur in a variety of ways without limiting the functionality of the device. For example, using a Graphical User Interface ("GUI") the operator can employ a sequence of mouse clicks to initiate the authentication process. Also, a specific sequence of keystrokes, such as ALT-A or some other combination can initiate the process. It is important to note that the

In operation 810, GPS time and date data is received and stored in temporary memory. In one embodiment, the GPS receiver is activated and the time and date are obtained, as described previously, and stored in a temporary memory area on the User Card. Referring to Figure 6, the User Card 410 includes a temporary memory 624 that is used to temporarily store summary data. The data in the temporary memory 624 is incorporated into the regular memory of the User Card 410 once authentication of the user has been completed by the challenge/response process that occurs between the User Card 410 and the System Card 600. In operation, time, date, location, device id, User Card id, newly calculated random number and the current measured delay number are all stored in the temporary memory 624 on the User Card 410. Once authentication has been established, the user is granted access to data that resides behind the System Card 600. Alternatively, a local Digital Certificate is created for later authentication as described in greater detail subsequently with reference to Figures 9 and 10.

In operation 812, the User Card 410 calculates the geophysical location of the client computer 409 using the GPS timing signals received by the GPS antenna 412. The User Card 410 uses the GPS timing signals to determine the precise geophysical location at that moment, and the geophysical location 628 is stored in temporary memory 624. Since the motion of the GPS satellites is highly complex, duplication of such timing signals by a fake source is essentially unfeasible.

A delay stack offset is determined and the delay number located at the stack offset in the client delay stack is copied to temporary memory, in operation 814. As shown in Figure 6, the client delay stack 614 includes a plurality of delay numbers. In operation 814, an offset into the client delay stack 614 is determined via a random number or other

A stack offset is determined and the previously stored random number located at the client random number stack offset in the client random number stack is copied to temporary memory, in operation 820. As shown in Figure 6, the client random number stack 612 includes a plurality of previously stored random numbers. In operation 820, an offset into the client random number stack 612 is determined, and the offset is then used to index the previously stored random number located at the offset within the client random number stack 612. The selected previously stored random number 634 is then copied to the temporary memory 624.

Referring back to Figure 8, a new random number is generated and pushed onto the client random number stack 612, in operation 822. The new random number can be generated by well known techniques that will be apparent to those skilled in the art. Post process operations are performed in operation 822. Post process operations can include creating a Digital Certificate using the obtained summary information, authenticating a transaction using the obtained summary information, and other post process operations that will be apparent to those skilled in the art. The process described in Figure 8 is meant to be instructive. It will be apparent to those skilled in the art that the selection of the delay and random numbers that are copied into temporary memory need not be limited to one each. Multiple randomly selected entries from the random number stack as well as multiple randomly selected delay numbers from the delay number stack can be employed as part of the creation of the summary information, further strengthening the integrity of the process by raising the complexity and entropy higher.

Figure 9 is a flowchart showing a method 900 for creating a Digital Certificate using obtained client summary information, in accordance with an embodiment of the

The Digital Certificate is then created in operation 910. The client public key 616 is used in conjunction with the client private key 618 to encrypt the summary data in the temporary memory 624 using PKI dual key encryption. The resulting Digital Certificate can then attest to the time, date, location, user, processor ID, receiver ID, new delay number, and new random number. If a hash code of the related document was created in operation 908, the hash code can be used subsequently to detect any changes to the related document content since certification. Post process operations are then performed in operation 912.

Post process operations include storing the Digital Certificate and related file on a storage medium, subsequent authentication operations, and other post process operations that will be apparent to those skilled in the art. In addition to facilitating Digital Certificate creation, the summary data can be used in transactions wherein a transmission is to occur, as discussed in greater detail next with reference to Figure 10.

Figure 10 is flowchart showing a method 1000 for authenticating a remote transaction, in accordance with an embodiment of the present invention. In an initial operation 1002, preprocess operations are performed. Preprocess operations include establishing a connection with a remote server computer, commencing the transaction application, and other preprocess operations that will be apparent to those skilled in the art.

In operation 800, summary data including GPS entropy data is obtained. Summary data is obtained as discussed previously with respect to method 800 of Figure 8. The obtained summary data is stored in temporary memory 624 and the client random number stack 612 and the client delay stack 614 are updated as discussed above.

In operation 1012, the System Card requests a mobile passphrase for the user. More specifically, the System Card encrypts a token using the system default private key and the client's public key. When decrypted, the contents of the token request that the User Card challenge the user for his/her mobile passphrase. The User Card issues a request to the Host Processor and the user is presented with a dialog box requesting that the mobile passphrase that was established during initialization be entered. The passphrase entered by the user is then returned to the User Card, which encrypts the response into a token using the system default public key and its client private key. Upon receipt, the System Card decrypts the token and compares the passphrase against the passphrase stored in the user's profile.

When the geophysical location data for the user does not match the profile, the transaction can still be authenticated if the user is approved for mobile access. Hence, in operation 1012, the user is prompted for their mobile passphrase. A decision is then made as to whether the mobile passphrase matches the mobile passphrase stored in the user's profile, in operation 1014. If the mobile passphrase matches the mobile passphrase stored in the user's profile, the method 1000 continues with operation 1018. Otherwise, the method 1000 continues with an authentication failure operation 1016. In the authentication failure operation 1016, access to the server computer is denied and the system administrator is notified to take any subsequent actions that have been instituted by the organization.

In operation 1018, a decision is made as to whether the remainder of the summary data included in the digital token matches the data included in user's profile. For example, the client ID and receiver ID can be validated. In addition, the delay number

the new system public key 620 in conjunction with the client private key 618. Referring back to Figure 10, the encrypted updated summary data is transmitted to the server computer in operation 1026. The server computer then uses the system private key 622 to decrypt the summary data and compares the summary data to the data included in the user's profile 606.

A decision is then made as to whether the received summary data, excluding the new delay and random numbers, matches the data stored in the user's profile, in operation 1028. If the summary data, excluding the new delay and random numbers, matches the data stored in the user's profile, the method 1000 continues with operation 1030. Otherwise, the method branches to the authentication failure operation 1016.

In operation 1030, the new delay number and the new random number included in the updated summary data are pushed onto the system stacks. Referring to Figure 6, the new delay number 630 included in the updated summary data 624 is pushed onto the system delay stack 610. Similarly, the new random number 634 included in the updated summary data 624 is pushed onto the system random number stack 608.

Referring back to Figure 10, a symmetric encrypted channel is then opened in operation 1032. A high speed symmetric encrypted channel is opened between the client computer 410 and the server computer 600. High speed encrypted communication is then permitted using a secure encryption technique, such as Security Sockets Layer (SSL), Data Encryption Standard (DES), Rijndael, or any other high speed encryption technique known to those skilled in the art.

The geo-location 628 is the physical location of the client computer as determined using external timing signals, such as GPS technology. As described above, the GPS system is a set of 24 satellites launched by the U.S. Department of Defense that are configured to facilitate identifying earth locations. The satellites of a GPS system provide timing signals, usually broadcast at 1.57 Ghz, that are received by the User Card through the GPS antenna. Although the following description is in terms of GPS technology, it should be noted that any external timing signals can be utilized by the embodiments of the present invention.

Embodiments of the present invention can also base the environmental profile 1100 on a pre-set association of a multiplicity of disk drives, each with a unique ID 1102, to a multiplicity of addresses. These addresses may be geo-location addresses, possibly unique for each drive, or may be physical electronic device addresses 1104 of each drive as it is configured to operate within a bank of other disk drives. Of course some combination of these is also envisioned by this disclosure. Hence, the disk on which the protected file resides is intimately tied to the protected file and the user's location. As a result, if the drive is replaced or the file is copied to another device, the protected file will become unreadable.

The environmental profile 1100 can be further based on a time and date range 1106. The time range 1106 can define a range of time and dates wherein the file may be accessed. Since the embodiments of the present invention obtain time information from external timing signals, such as the GPS system, users cannot "spoof" the system by altering their system, or other internal clock. As can be seen, when the external timing signal no longer indicates a time or date within the given time or date range 1106, the

Figure 13 is a flowchart showing a method 1300 for protecting electronic files based on location, in accordance with an embodiment of the present invention. In an initial operation 1302, preprocess operations are performed. Preprocess operations include establishing a connection with a remote server computer, commencing the transaction application, and other preprocess operations that will be apparent to those skilled in the art.

In operation 800, summary data including GPS entropy data is obtained. Summary data is obtained as discussed previously with respect to method 800 of Figure 8. The obtained summary data is stored in temporary memory 624 and the client random number stack 612 and the client delay stack 614 are updated as discussed above.

A digital token is created in operation 1304. The User Card uses the system default public key in conjunction with the client private key to encrypt the summary data stored in the temporary memory into a digital token. For example, the summary data can include the GPS time and date, the calculated geophysical location, the selected previously stored delay number, the selected previously stored random number, the client ID, and the receiver ID. It should be borne in mind that the digital token is not required to include all the information stored in temporary memory. In some embodiments, some amount of summary information less than all the information shown in the temporary memory mentioned above is encrypted into the digital token.

The digital token is transmitted to the server computer in operation 1306. Upon receipt, the server computer decrypts the digital token, in operation 1308. The server computer decrypts the digital token using the system default private key. The server

transmitted to the client computer 410, in operation 1322. In further embodiments of the present invention, operation 1320 can be performed after a fully authenticated communication channel has been established. In such embodiments, operation 1320 can follow operation 1032 of Figure 10.

In response to receiving and decrypting the request 1400 for the environment profile, the client computer generates a new client key pair, in operation 1324. Turning to Figure 14, the client computer 410 generates both the new client public key 1202 and new client private key 1204 based on the user's passphrase 602 and the environment profile 1100, as described above with reference to Figure 12. In addition, embodiments of the present invention can also store a key pair hash code 1402, which is a number hashed from the passphrase 602 and the environment profile 1100. The key pair hash code 1402 can later be used to check the operating environment during future file access, as described in greater detail subsequently. The new client public key 1202 is then encrypted using the new system public key 638 and the new client private key 1204, and transmitted to the server computer 600 in operation 1326.

Referring back to Figure 13, the server computer encrypts the payload using the new client public key, in operation 1328. As shown in Figure 14, the server computer 600 encrypts the payload 1404, which is the electronic data being protected, using the new client public key 1202 and the new system private key 1406. The encrypted payload 1404 is then transmitted to the client computer 410, in operation 1330.

Post process operations are performed in operation 1332. Post process operations can include user access to the encrypted payload data file, further file transmissions, and other post process operations that will be apparent to those skilled in the art. Since the

environment profile that represents the current operating environment of the client computer.

In operation 1508, the passphrase and the appended current environment profile are hashed to create a current key hash code. As mentioned above, embodiments of the present invention process the passphrase and the appended environment profile to generate the new client public and private key pair, which is used for file encryption. In addition, during the new client key pair creation, the hash code based on the new client public and private key pair and environment profile can be saved. This saved original key pair hash code can be used for verification.

A decision can then be made as to whether the current key pair hash code matches the original key pair hash code, in operation 1510. If the current key pair hash code does not match the original key pair hash code, the method 1500 fails in operation 1512. Hence, the file access can fail because of a change in the operating environment as well as by entering the wrong passphrase. If the current key pair hash code matches the original key pair hash code, the method 1500 continues with a decrypting operation 1514.

In decrypting operation 1514, the encrypted payload data file is decrypted using the new client private key. Hence, if the expected operating environment is maintained at the time of file access, the new client private key is used to decrypt the data file. In a further embodiment of the present invention, the passphrase and appended current environment profile are used to generate another new client private key. This client private key is then used to decrypt the payload data. However, the movement, removal, or re-arrangement of one or more environment variables will cause the composition of the environment profile to change, thereby creating an incorrect private key for use in the